



**PREP
SCHOOLS
TRUST**

Records Retention and Deletion Policy

Owner:	Data Compliance Lead	Date Reviewed:	July 2023
---------------	-----------------------------	-----------------------	------------------

Review Period:	1 Year	Next Review Date:	July 2024
-----------------------	---------------	--------------------------	------------------

RECORDS RETENTION AND DELETION POLICY

1. INTRODUCTION

- 1.1. The main aim of this policy is to enable Prep Schools Trust (“the **Trust**”) to manage its records effectively and in compliance with data protection law, namely: the UK General Data Protection Regulation (“**UK GDPR**”), the Data Protection Act 2018 (“**DPA 2018**”) and other related legal and regulatory requirements.
- 1.2. In this policy, the term ‘school(s)’ means Barfield, Chandlings Prep, Cothill House, Kitebrook and Mowden Hall. For the avoidance of doubt, the Trust is the data controller for all the schools governed and administered by the Trust and this policy is therefore intended to be written on behalf of all the schools in the Trust.
- 1.3. This policy applies to all our staff, including employees, trustees, volunteers, peripatetic staff, interns, consultants, external contractors, temporary workers, agency workers and casual workers. All such persons must understand and comply with this policy. Failure to do so may subject us, and/or our workforce to civil and/or criminal liability. Any failure to comply with this policy may result in disciplinary sanctions, including suspension or termination of a contract.
- 1.4. The Trust collects, holds, and creates significant amounts of data and information. This policy explains the Trust’s requirements to retain certain information and provides guidance on appropriate disposal.
- 1.5. This policy covers all data that the Trust holds or has control over. This includes physical data such as hard copy documents, contracts, notebooks, letters and invoices. It also includes electronic data such as emails, electronic documents, and audio and video recordings. It applies to both personal data and non-personal data. In this policy we refer to this information and these records collectively as “data”.
- 1.6. This policy also covers data that is held by third parties on the Trust’s behalf, for example cloud storage providers. It also extends to data that belongs to us but is held by employees or volunteers on their personal devices (e.g. personal mobile phones) information security policy and our bring your own device (“BYOD”) policy.
- 1.7. We are committed to the principles of data protection including the principle that personal data is only to be retained for as long as necessary for the purpose for which the data is processed (the ‘storage limitation’ principle).
- 1.8. The Data Compliance Lead, Jo Fitzroy-Ezzy, is responsible for overseeing the implementation of this policy and for monitoring our compliance. If you have any concerns or questions regarding retention of data or data disposal or need to report non-compliance, please contact the Data Compliance Lead via datacompliance@prepschoolstrust.org or 01865 390720.

2. TYPES OF DATA

- 2.1. **Retention Schedule data:** Certain types of data that we routinely process are listed in the Retention Schedule in the Appendix. There are various reasons why we retain this data, for example, we may have a legal requirement to retain it, or we may need it in order to provide education to our pupils.
- 2.2. **Disposable data:** Disposable (day-to-day) data consists of data that serves only a temporary purpose and is not a part of any formal or official record included in the Retention Schedule. Such data should be deleted or discarded by the user once it has served its temporary purpose (please see the Appendix below for more information on retention of this type of data).

Examples of disposable data include:

- 2.2.1. duplicates of originals that have not been annotated;
 - 2.2.2. preliminary drafts of documents that do not represent significant steps or decisions and are not required to be retained;
 - 2.2.3. manuals, training materials and other printed materials obtained from sources outside of the Trust and retained for reference purposes;
 - 2.2.4. spam and junk mail and day-to-day emails that are no longer relevant to the needs of the Trust.
- 2.3. **Personal data:** Both Retention Schedule data and Disposable data may contain personal data (i.e. data that identifies or is capable of identifying living individuals). Data protection laws require us to retain personal data for no longer than is necessary for the purposes for which it is processed (this is known as the principle of storage limitation). See the Appendix and paragraph 4 below for more information on retention periods for personal data.

3. PRINCIPLES OF DATA RETENTION

- 3.1. Through our data retention practices, we aim to meet the following commitments:
- 3.1.1. comply with relevant legal and regulatory requirements to retain data;
 - 3.1.2. comply with our data protection obligations;
 - 3.1.3. handle, store and dispose of data responsibly and securely;
 - 3.1.4. create and retain data where we need this to operate the Trust and its schools' effectively, but not create or retain data without good reason;
 - 3.1.5. allocate appropriate resources and responsibilities to data retention, regularly monitor compliance with this policy and update this policy when required.

4. DOCUMENT RETENTION PERIOD

- 4.1. The Retention Schedule contained in the Appendix sets out the categories of data that we hold, the length of time that we need to retain them, and the reason for this.
- 4.2. Any data that is part of any of the categories listed in the Retention Schedule, must be retained for the relevant amount of time indicated in the Retention Schedule. It must not be retained beyond the period indicated in the Retention Schedule, unless a valid reason (including notice to preserve documents for contemplated litigation or other special situation - see paragraph 7 below) calls for its continued retention.
- 4.3. Where personal data is listed in the Retention Schedule, we have considered the principle of storage limitation and balanced this against our requirements to retain the data.
- 4.4. The Retention Schedule does not set out retention periods for Disposable data. This type of data should only be retained for as long as it is needed. Once it no longer has any value to the Trust, it should be securely disposed of. Where personal data is disposable information, you must consider the principle of storage limitation when deciding whether to retain this data.

- 4.5. If data is not listed in the Retention Schedule, it is likely that it should be classed as disposable data. However, if you consider that there is an omission in the Retention Schedule, or if you are unsure whether to retain a certain record, contact the Data Compliance Lead for further guidance.

5. STORAGE AND BACK-UP OF DATA

- 5.1. Our data must be stored in a safe, secure, and accessible manner.
- 5.2. All documents should be duplicated or backed up regularly. The Trust uses Google who handles the backing up of its servers and data is not saved on site as it's all in the cloud. All of our sites use Google Vault which keep a copy of any document created within the google system.
- 5.3. The Trust may use external providers for systems to store and manage data which includes iSAMS for parent data which is cloud based. Details on these systems and their security procedures can be found in our Trust Wide Systems and Data Protection and Security document.
- 5.4. If a document has reached the end of its stated retention period, but you are of the view that it should be retained for longer, please refer to the School or Trust Data Compliance Lead, who will decide whether it should be retained, for how long, and note the new time limit and reasons for extension.

6. DISPOSAL OF DATA

6.1. General

- 6.1.1. When a document reaches the end of its retention period, it should be deleted / disposed of in accordance with this policy.
- 6.1.2. It may be necessary to delete certain personal data before the end of the retention period in response to a request for erasure. Any such requests should be forwarded to the Data Compliance Lead who will decide how to proceed.
- 6.1.3. The Data Compliance Lead is responsible for the process of identifying the data that has reached its retention period and its safe destruction.

6.2. Confidential waste

- 6.2.1. The destruction of confidential data (confidential documents will include financial, staff and workforce-related records, and other documents containing sensitive information) must be conducted securely. i.e. in such a way that it cannot be read or reconstituted.
- 6.2.2. In the case of manual records such as paper records, these should be securely shredded (i.e. using a cross-cutting shredder).
- 6.2.3. In the case of digital storage devices such as DVDs, these should be securely cut and hard discs ground down.
- 6.2.4. Any records that contain personal data or special category personal data should be treated as confidential.

6.3. Non-confidential data

6.3.1. Non-confidential hard copy data may be destroyed by recycling.

6.4. Electronic data

6.4.1. The destruction of electronic data must be overseen by the Data Compliance Lead who will decide whether the relevant data should be deleted irretrievably, archived or (in cases where permanent deletion is temporarily impossible for technical reasons) 'put beyond use' (with appropriate safeguards in place and commitment for permanent deletion, when it becomes possible).

6.5. Routine deletion

6.5.1. Certain data may be routinely archived by the computer systems. Should you want to retrieve any information, or prevent this happening in a particular circumstance, please contact the Data Compliance Lead or Head of IT.

6.5.2. You should always consider the following factors when deciding on retention or disposal:

- 6.5.2.1. has the information come to the end of its useful life?
- 6.5.2.2. is this data included in the Retention Schedule? Is there a legal requirement or other justification to keep this data and if so, for what period? (Refer to the Appendix for more information.)
- 6.5.2.3. would this data be likely to be needed in the case of any legal proceedings? (Is the information contentious, does it relate to an incident that could potentially give rise to legal proceedings?)
- 6.5.2.4. would the document be useful for the Trust as a precedent, learning document, or for performance management processes?
- 6.5.2.5. is the document of historic or statistical significance? If it includes personal data, is it possible to retain it in an anonymised or pseudonymised form?
- 6.5.2.6. are there any special circumstances set out in paragraph 7 below?

7. SPECIAL CIRCUMSTANCES – PRESERVATION OF DOCUMENTS

7.1. The destruction of data must stop immediately if you believe, or you are informed that certain records may be relevant to current litigation or contemplated litigation (that is, a dispute that could result in litigation), government investigation, audit, or any other event. In such circumstances, you must preserve and not delete, dispose, destroy, or change those records, including emails and other electronic documents, until the Data Compliance Lead determines those records are no longer needed. Preserving documents includes suspending any requirements in the Retention Schedule and preserving the integrity of the electronic files or other format in which the records are kept.

7.1.1. If you believe this exception may apply, or have any questions regarding whether it may apply, please contact the Data Compliance Lead.

7.2. You may be asked to suspend any routine data disposal procedures in connection with certain other types of events, such as receipt of a data subject request, a restructure or the replacement of our information

technology systems. Destruction may begin again once the Data Compliance Lead lifts the requirement for preservation.

- 7.3. Under the terms of the Independent Inquiry into Child Sexual Abuse (“IICSA”), it is an offence to destroy any records that might be of relevance to the inquiry. This overrides any other requirements, including rights of a data subject under the UK GDPR. If you believe that the records held (either relating to staff or pupils) relate to the inquiry, then they must be retained indefinitely and the Trust should ensure that these records are kept securely and are not deleted. Please see the [guidance note](#) produced by IICSA for further information.

8. OTHER RELEVANT POLICIES

- 8.1. This policy supplements and should be read in conjunction with our other policies and procedures in force from time to time, including information about your legal rights in Part 2 ‘Data Subject Rights Policy’ contained within our Data Protection Policy, the Information Security Policy, and the Acceptable Use / BYOD Policy.

You can find out more information about your legal rights in Part 2 ‘Data Subject Rights Policy’ contained within our Data Protection Policy which can be found on the [intranet](#) and our website.

APPENDIX

Trust specific records

Information Type	Statutory basis for retention	Retention period	Action after retention period ends
Corporate records			
Governing documents	Companies Act 2006 Charities Act 2011	Permanent (or until closure of the Trust)	Secure disposal
Minutes of Trustee meetings and written resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years	Secure disposal
Members' meetings etc. Minutes / resolutions	Companies Act 2006 Charities Act 2011	Recommended at least 10 years	Secure disposal
Scheme of delegation and terms of reference for committees		To be retained until superseded.	Secure disposal
Trustee Management			
Records relating to the appointment of a Clerk to the Trustees	Limitation Act 1980	Date on which clerk appointment ceases + 6 years	Secure disposal
Records relating to Trustee declaration against disqualification criteria	Limitation Act 1980	Date appointment ceases + 6 years	Secure disposal
Register of business interests	Limitation Act 1980	Date appointment ceases + 6 years	Secure disposal
Code of Conduct		Permanent (or until closure of the Trust)	Secure disposal

Records relating to the training required and received by Trustees	Limitation Act 1980	Date appointment ceases + 6 years	Secure disposal
Individual Trustee personnel files (and members of local governing bodies)	Limitation Act 1980	Date appointment ceases + 6 years	Secure disposal
Operational Management of the Trust and its schools			
Log books of activity in each school maintained by the relevant Head Teacher		Retain for a minimum of 6 years from the date of last entry in the book	Secure disposal
Senior Management Team meetings minutes		Retain for a minimum of 3 years then review as required	Secure disposal
Reports created by the relevant Head Teacher or Senior Management Team of each school		Retain for a minimum of 3 years then review as required	Secure disposal
Individual school development plans		Life of the plan + 3 years	Secure disposal
Policies and privacy notices	Limitation Act 1980	Until superseded + 6 years	Standard disposal
Newsletters and other items with a short operational use		Current academic year + 1 year	Standard disposal
Visitor management systems (including electronic systems, visitors' books and signing-in sheets)		Last entry in the visitors' book + 6 years (in case of claims by parents or pupils about various actions).	Secure disposal
Commercial			
Contracts e.g. with suppliers or grant makers	Limitation Act 1980	Duration of contract term plus 6 years	Secure disposal

Contracts executed as deeds	Limitation Act 1980	Duration of contract term plus 12 years	Secure disposal
Intellectual Property records and legal files regarding provision of service	Limitation Act 1980	Life of service provision or IP plus 6 years	Secure disposal
Taxation and finance			
Annual accounts and review (including transferred records on amalgamation)	Companies Act 2006 Charities Act 2011	Minimum 6 years	Secure disposal
Tax and accounting records	Finance Act 1998 Taxes Management Act 1970	6 years from end of relevant tax year	Secure disposal
Information relevant for VAT purposes	Finance Act 1998 and HMRC Notice 700/21	Minimum 6 years from end of relevant period	Secure disposal
Banking records / receipts book/sales ledger	Companies Act 2006 Charities Act 2011	6 years from transaction	Secure disposal
Insurance			
Employer's Liability Insurance	Employers' Liability (Compulsory Insurance Regulation) 1998	Closure of the school + 40 years	Secure disposal. To be passed to the Local Authority on closure.
Policies	Commercial	3 years after lapse	Secure disposal
Claims correspondence	Commercial	3 years after settlement	Secure disposal
Property			
Original title deeds		Permanent / to disposal of property	Secure disposal
Leases	Limitation Act 1980	12 years after lease has expired	Secure disposal

Building records, plans, consents and certification and warranties etc	Limitations Act 1980	6 years after disposal or permanent if of historical / archival interest.	Secure disposal
Health and safety			
Health and safety policy statements		Life of policy + 3 years	Secure disposal
Health and safety risk assessments		Life of risk assessment + 3 years provided that a copy of the risk assessment is stored with the accident report if an incident has occurred	Secure disposal
Accident reporting records relating to individuals	Social Security (Claims and Payments) Regulations 1979 Regulation 25 Social Security Administration Act 1992 Section 8. Limitation Act 1980	The Accident Book – BI 510 – minimum of 3 years after last entry in the book	Secure disposal
Records relating to any reportable death, injury, disease or dangerous occurrence (RIDDOR)	Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 SI 2013 No 1471 Regulation 12(2)	Date of incident + 3 years provided that all records relating to the incident are held on an individual's personnel file Note: any safeguarding incident (e.g. abuse) will be retained indefinitely for the purposes of the IICSA. Thereafter they will be retained for duration of any living victim (Limitation Act 1980).	Secure disposal

Control of Substances Hazardous to Health (COSHH)	Control of Substances Hazardous to Health Regulations 2002, Regulation 11. Records kept under the 1994 and 1999 Regulations to be kept as if the 2002 Regulations had not been made. Regulation 18 (2)	Date of incident + 40 years	Secure disposal
Process of monitoring of areas where employees and persons are likely to have come into contact with asbestos	Control of Asbestos at Work Regulations 2012 SI 1012 No 632 Regulation 19	Last action + 40 years	Secure disposal
Process of monitoring of areas where employees and persons are likely to have come into contact with radiation.	The Ionising Radiation Regulations 2017. SI 2017 No 1075 Regulation 11 As amended by SI 2018 No 390 Personal Protective Equipment (Enforcement) Regulations 2018	2 years from the date on which the examination was made and that the record includes the condition of the equipment at the time of the examination. Records relating to dose assessment and recording to be maintained until the person to whom the record relates reaches 75 years of age / 30 years from when the record was made.	Secure disposal
Fire Precautions log books		Current year + 3 years	Secure disposal
Health and safety file to show current state of building, including alterations		Permanent / to disposal of property	Transfer to the new owner of the property

Pupil records

Personal identifiers

Images used for identification purposes		For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Secure disposal
Images used for marketing purposes		For the duration of consent provided	Secure disposal
Biometric data		For the duration of the event/activity, or whilst the pupil remains at school, whichever is less, plus one month	Secure disposal
Admissions			
Records relating to the creation and implementation of the Admissions Policy		Life of the policy + 3 years then review	Secure disposal
Admission records (successful)		<p>Date of birth of the pupil + 25 years</p> <p>(recommended rather than IRMS guidance of 1 year due to the limitation period relating to some claims e.g. personal injury/negligence that a child can bring in their own right once they turn 18 years old. By retaining the records for this duration means the Trust would then have documentation in which to respond to any claim.)</p>	Secure disposal

Admission records (unsuccessful applicants) e.g. application forms, assessments and records of decisions		Minimum of 6 months	Secure disposal
Admissions Register	Pupil Registration Regulations 2006 Regulation 14	Each entry in the admission register must be preserved for a period of three years after the date on which the entry was made	Secure disposal
Educational records			
Educational Records	Limitation Act 1980	The file should follow the pupil when they leave the primary school. Some information may be retained from date of birth of the pupil + 25 years in order to respond to a complaint / defend a claim.	Transfer to new school / secure disposal
Child protection information held on pupil file	Keeping Children Safe in Education statutory guidance for schools and colleges Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018	Date of birth of the pupil + 25 years* If any records relating to child protection issues are placed on the pupil file, it should be in a sealed envelope and then retained for the same period of time as the pupil file. Note: These records will be subject to any	*File should transfer to the pupil's new school but is advised a copy is retained for the purposes of the Independent Inquiry into Child Sex Abuse (ICSA) Secure disposal

		instruction given by IICSA and currently will be retained indefinitely for the purposes of the Inquiry.	
Child protection information held in separate files	<p>Keeping Children Safe in Education statutory guidance for schools and colleges</p> <p>Working together to safeguard children. A guide to inter-agency working to safeguard and promote the welfare of children 2018</p>	<p>Date of birth of the pupil + 25 years*</p> <p>Note: These records will be subject to any instruction given by IICSA and currently will be retained indefinitely for the purposes of the Inquiry.</p>	<p>*File should transfer to the pupil's new school but is advised a copy is retained for the purposes of the Independent Inquiry into Child Sex Abuse (ICSA)</p> <p>Secure disposal</p>
SEN(D) files	Limitation Act 1980	<p>Date of birth of the pupil + 31 years (An Education, Health and Care Plan is valid until the individual reaches the age of 25 years, the retention period adds an additional 6 years from the end of the plan in line with the Limitation Act 1980).*</p>	<p>*File should transfer to the pupil's new school but is advised a copy is retained owing to the limitation period that can apply to certain claims an individual can bring.</p> <p>Secure disposal or transfer to the pupil's new school</p>

<p>Education Health and Care Plans</p>	<p>As applicable, Special Educational Needs and Disability Regulations 2014 and Children and Families Act 2014, Part 3</p>	<p>Date of birth of the pupil + 25 years*</p>	<p>*File should transfer to the pupil's new school but is advised a copy is retained owing to the limitation period that can apply to certain claims an individual can bring.</p> <p>Secure disposal or transfer to the pupil's new school</p>
<p>Statements of Special Educational Needs (now historic)</p>	<p>Originally under Special Educational Needs and Disability Regulations 2001 (as applicable)</p>	<p>Date of birth of the pupil + 25 years</p>	<p>*File should transfer to the pupil's new school but is advised a copy is retained owing to the limitation period that can apply to certain claims an individual can bring.</p> <p>Secure disposal or transfer to the pupil's new school</p>
<p>Attendance Registers</p>	<p>Pupil Registration Regulations 2006 Regulation 14</p>	<p>3 years from when the register entry was made if made in paper registers</p> <p>For computerised registers retain until 3 years after the end of the school year during which the entry was made. This applies to every back up copy.</p> <p>The difference in retention periods as between manual and computerised registers has probably come about in error but this is what the Regulations say.</p>	<p>Secure disposal</p>

Pupil subject access requests	Data Protection Act 2018	1 year following completion of the request	
Alumni			
Alumni records		For as long as there is an active relationship	Secure disposal

Parent records

Personal identifiers	Pupil Registration Regulations 2006 For basic name and contact details. Otherwise usually operational in accordance with the statutory functions of the school.	Usually, for the duration that the parent has a pupil at the school. Otherwise subject to case by case justification.	Secure disposal
Parental consent forms		Until the conclusion of the trip or if a major incident has occurred, to be retained in the pupil's record.	Secure disposal
Visitor logs		Last entry in the visitors' book + 6 years.	Secure disposal
Parent correspondence		To be retained for as long as necessary, for inclusion in the educational record where appropriate (e.g. records of absences).	Secure disposal

Parental subject access requests	Data Protection Act 2018	1 year following completion of the request	
----------------------------------	--------------------------	--	--

Staff records

Recruitment			
Applications (unsuccessful)	Equality Act 2010	6 months from your notification of outcome of application	Secure disposal
Applications (successful)		To be added to the personnel file and retained until end of appointment + 6 years, except in cases of negligence or claims of child abuse then at least 15 years (or permanent in line with IICSA)	Secure disposal
Pre-employment vetting information – DBS Checks – successful candidates	DBS Update Service Employer Guide June 2014; Keeping Children Safe in Education 2021	Applications forms, references and other documents – for the duration of the employee’s employment + 6 years	Secure disposal
Forms of proof of identity collected as part of the process of checking “potable” enhanced DBS disclosure	Keeping Children Safe in Education 2021	Where possible this process should be carried out using the on-line system. If it is necessary to take a copy of documentation then it should be retained on the staff personnel file.	Secure disposal

		DBS disclosures, if held, to be retained for no longer than 6 months from decision on recruitment.	
Pre-employment vetting information – Evidence proving the right to work in the United Kingdom – successful candidates	An Employer’s Guide to Right to Work Checks (Home Office, May 2015)	Where possible these documents should be added to the staff personnel file, but if they are kept separately then the Home Office requires that the documents are kept for termination of employment + not less than 2 years.	Secure disposal
Note: A permanent record will be kept of all mandatory checks on the Single Central Register (but not the DBS certificate itself).			
Employee personnel files			
Income tax and NI returns, income tax records and correspondence with HMRC.	The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended	Not less than 3 years after the end of the financial year to which they relate.	Secure disposal
Payroll wage/salary records (also overtime, bonuses, expenses)	Taxes Management Act 1970	6 years from the end of the tax year to which they relate.	Secure disposal
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence (also shared parental, paternity and adoption pay records)	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended, Maternity & Parental Leave Regulations 1999.	3 years after the end of the tax year in which the maternity period ends	Secure disposal

Sick pay	Statutory Sick Pay (General) Regulations	3 years after the end of the tax year	Secure disposal
National Minimum wage records	National Minimum Wage Act 1998	3 years after the end of the pay reference period following the one that the records cover	Secure disposal
Foreign national ID documents	Immigration (Restrictions on Employment) Order 2007 Independent School Standards Regulations	Minimum 2 years from end of employment	Secure disposal
HR files and training records	Limitation Act 1970 and Data Protection regulation	Maximum 6 years from end of employment. Note: any information which may be relevant to the IICSA may be retained for the purposes of the Inquiry.	Secure disposal
Working time records including overtime, annual holiday, jury service, time off for dependents, etc	Working Time Regulations 1998 as amended	2 years	Secure disposal
Coronavirus Job Retention Scheme (records of the furlough agreement, including the amount claimed, claim period for each employee, claim reference number and calculations in case HMRC need more information)	Statutory guidance 'Claim for wages through the Coronavirus Job Retention Scheme'	6 years for furlough records (employers should retain the written furlough agreement for 5 years. But HMRC can retrospectively audit all claims so it is important to keep a copy of all	Secure disposal

		records for 6 years minimum.)	
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	The Retirement Benefits Schemes (Information Powers) Regulations 1995	6 years from the end of the scheme year in which the event took place	Secure disposal
Staff subject access requests	Data Protection Act 2018	1 year following completion of the request	Secure disposal
Whistleblowing documents	Public Interest disclosure Act 1998 and recommended IAPP practice.	6 months following the outcome (if a substantiated investigation). If unsubstantiated, personal data should be removed immediately.	Secure disposal
Pension records		12 years after the benefit ceases.	